

US DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
FILED

UNITED STATES DISTRICT COURT

JUN 08 2018

for the

Western District of Arkansas

DOUGLAS F. YOUNG, Clerk
By

Deputy Clerk

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Yahoo! Email Account/ User ID
sgttalbertmill@yahoo.com stored at Oath Holdings Inc.

Case No.

2:18CM 10

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Western District of Arkansas, there is now concealed (identify the person or describe the property to be seized):

This court has authority to issue this warrant under 18 U.S.C. § 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41. See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 641	Theft of Government Funds
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 287	False Claim for Tax Refund

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Greg Alexander
Applicant's signature

Greg Alexander, Special Agent IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date:

6/8/18

Erin L. Wiedemann
Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, U.S. Magistrate Judge
Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Gregory Alexander, being first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require the provider listed in Attachment A (the provider) to provide information, including the content of communications, for the email accounts listed in Attachment A, including user names and associated profiles. As set forth below, I have probable cause to believe that these accounts contain evidence, as set forth in Attachment B to this affidavit, of violations of the following:
 - a. 18 USC § 287, False Claims for Tax Refund
 - b. 18 USC § 641, Theft of Public Money
 - c. 18 USC § 1028A, Aggravated Identity Theft
2. I am a Special Agent with the Internal Revenue Service Criminal Investigation, and have been so employed since October 2001. As a Special Agent, I investigate possible violations of the Internal Revenue Code (Title 26 United States Code), the Money Laundering Control Act (Title 18 United States Code), the Bank Secrecy Act (Title 31 United States Code) and other criminal violations. I have personally conducted and assisted other law enforcement officers in numerous investigations of alleged criminal violations of the Internal Revenue Laws, the Bank Secrecy Act, and the Money Laundering Control Act.
3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own knowledge, knowledge obtained from other

individuals during my participation in this investigation, including other IRS personnel, interviews of witnesses, analysis of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

APPLICABLE LAW

4. Title 18 U.S.C. § 287 (False, Fictitious, or Fraudulent Claims) provides in relevant part that
“whoever makes or presents to any person or officer in the civil, military, or naval services of the United States, or to any department or agency thereof, any claim upon or against the United States, or any department or agency thereof, knowing such claim to be false, fictitious, or fraudulent, shall be imprisoned not more than five years and shall be subject to a fine in the amount provided in this title.”
5. Title 18 U.S.C. § 641 (Public Money, Property, or Records) provides in relevant part that
“Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys, or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined, or converted – shall be fined under this title or imprisoned not more than ten years, or both...”
6. Title 18 U.S.C. § 1028A (Aggravated Identity Theft) provides in relevant part that
“Whoever, during and in relation to any felony violation enumerated in subsection (c) [18 U.S.C. §641, Public Money, Property, or Records, 18 U.S.C. § 1343, Wire Fraud] knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another

person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.”

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A) and 2711. Specifically, pursuant to 18 U.S.C. 2711 (3)(A)(i) the Court is “a district court of the United States....that has jurisdiction over the offense being investigated.” Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

STATEMENT OF PROBABLE CAUSE

8. In or around October 2016, information was received by the Internal Revenue Service Criminal Investigation (IRS-CI), Nashville Field Office, Fayetteville Post of Duty, related to suspicious financial activity on the part of an individual who will be referred to as B.H. and members of her family (collectively the B.H. family). The information pertained to, among other things, income tax refunds issued in various names deposited to bank accounts owned by the B.H. family.
9. I obtained and analyzed bank account records of the B.H. family¹ from Subiaco Federal Credit Union, Arvest Bank, First National Bank, and Logan County Bank. Analysis of these bank records revealed deposits of income tax refunds in names other than the B.H. family. The bank account numbers were queried against IRS databases to identify income tax returns that directed refunds to these bank accounts. Additionally, records were obtained from EPS

¹ Included in this was one non-family member who was a friend of the family.

Financial, Republic Bank and Trust, Santa Barbara Tax Products Group², Drake Software, Tax Act, Tax Hawk, and Intuit.³ The analysis of these records to date has identified 91 federal income tax returns in different taxpayers' names that were filed, or attempted to be filed, with the IRS from April 2013 to April 2016. These 91 federal income tax returns all claimed income tax refunds that were directed to be deposited to bank accounts owned by the B.H. family. To date, the investigation has identified \$613,827 in total refunds claimed, with an actual loss to the IRS of \$89,756.

10. Analysis is currently being performed on these tax returns. To date, however, 66 of these income tax returns have been determined to be fraudulent according to IRS records. Additionally, IRS-CI Special Agents have conducted interviews with eight taxpayers associated with six of the tax returns. All eight of the taxpayers confirmed that the income tax returns in question were fraudulent, and they did not file the tax returns.
11. I interviewed B.H. seven times between May 16, 2017 and July 6, 2017. B.H. stated she met a man online on May 6, 2012 whom she knew as JOHNSON MORRISON WILLIAMS (WILLIAMS). WILLIAMS said he was a Captain in the U.S. Army stationed in Afghanistan. B.H. was in a "relationship" with WILLIAMS from May 2012 until 2016, and they mainly communicated via Yahoo! email and chat. B.H. spoke to WILLIAMS a few times on the phone, but never met him in person.
12. During this time, WILLIAMS had money deposited to the B.H. family bank accounts, and had B.H. and some of her family members open new bank accounts. WILLIAMS told B.H. that the money being deposited to their accounts was from friends, and the money was to pay for WILLIAMS' expenses and assist him in securing leave. B.H. was unaware that income

² EPS Financial, Republic Bank and Trust, and Santa Barbara Tax Products Group are companies that provide refund transfer products and services that process tax preparation fees from the tax refunds.

³ Drake Software, Tax Act, Tax Hawk, and Intuit are tax preparation software companies.

tax refunds in other peoples' names were deposited to the B.H. family bank accounts. Once the money was deposited to the B.H. family bank accounts, WILLIAMS instructed B.H. on where to send the money. The money was sent via Western Union, MoneyGram, or bank transfer. Much of the money was sent to recipients in Nigeria. Based upon my training and experience, I recognized B.H. as a "romance scheme" victim being used in a Stolen Identity Refund Fraud (SIRF) scheme.

13. B.H. communicated with WILLIAMS at one of two email accounts. She first communicated with WILLIAMS at the email address jmorriswill48@yahoo.com, but at some point the email address changed to c.jmorriswill48@yahoo.com. On July 19, 2017, a federal search warrant was obtained in the Western District of Arkansas for jmorriswill48@yahoo.com and c.jmorriswill48@yahoo.com. The search warrant was served on Yahoo! Inc. on July 19, 2017.
14. I subsequently received and analyzed records from Yahoo! Inc. pursuant to the search warrant. This analysis identified dozens of email addresses that jmorriswill48@yahoo.com and c.jmorriswill48@yahoo.com had communicated with since 2012 related to romance schemes and/or SIRF schemes. Some of these email addresses appeared to be those of additional romance scheme victims, and some appeared to be those of co-conspirators. One of these email addresses of a suspected co-conspirator was patrobertson501@yahoo.com.
15. 96 emails and numerous chats were exchanged between patrobertson501@yahoo.com and c.jmorriswill48@yahoo.com from February 7, 2014 to July 10, 2017. Many of the emails and chats involved the passing of bank account information of known and suspected romance scheme victims, as well as information pertaining to income tax refunds that were expected to be deposited to bank accounts. Below are two examples of the email communication:

- a. As an example, on April 21, 2015, patrobertson501@yahoo.com sent the following email to c.jmorriswill48@yahoo.com:

“Arvest Bank
N.S.H.⁴
Account Name: N.S.H.
Account: Savings
Account Number: *****1381
Routing Number: 082900872.....
Federal Refund: \$8,851.....
SENDER IS.....J.O.S.”

On April 22, 2015, an \$8,816.02⁵ deposit in the name of J.S. (same first and last name as in the email where the sender is J.O.S., but without the middle name) was deposited to N.S.H.’s Arvest account ending in 1381. The federal income tax return which generated this refund was found to be fraudulent.

- b. On September 7, 2016, c.jmorriswill48@yahoo.com sent an email to patrobertson501@yahoo.com. This email contained images of a Citibank credit card in the name of M.B. I subsequently obtained the records from Citibank for this credit card. The application was dated August 17, 2016, and included the email address patrobertson501@gmail.com⁶. I interviewed M.B. on April 26, 2018, and she confirmed that she had not applied for the credit card and the email account was not hers.

16. On November 8, 2017, federal search warrants were obtained in the Western District of Arkansas for the email account patrobertson501@yahoo.com and others. The search warrant for Yahoo! Inc. was served on November 8, 2017.

⁴ N.S.H. is a member of the B.H. family.

⁵ The difference in the amount deposited and the amount in the email is due to \$34.98 in fees from the third party processor.

⁶ A preservation request was submitted to Google Inc. on December 18, 2017 requesting that they preserve all stored communications, records, and other evidence in their possession for 90 days. A 90 day extension was requested on March 13, 2018.

17. On or about February 2, 2018, I received documents pursuant to the search warrant on Yahoo! Inc. This included information for the email address patrobertson501@yahoo.com. Analysis of the patrobertson501@yahoo.com revealed communications with numerous email accounts related to SIRF schemes beginning in 2014. Many of these email addresses appeared to be with co-conspirators. Based upon my review of the email records of patrobertson501@yahoo.com, it appears that a primary use of this email account was to conduct romance schemes, SIRF schemes, and other identity theft schemes. Two of the email addresses of suspected co-conspirators are mic79@yahoo.com and sgttalbertmill@yahoo.com⁷.
18. On October 4, 2016, mic79@yahoo.com sent an email to patrobertson501@yahoo.com. This email contained images of a Citibank credit card in the name of K.S. I subsequently obtained the records from Citibank for this credit card. The application was dated August 16, 2016, and showed the credit card account was in the name of L.L. with an email address of patrobertson501@gmail.com. I interviewed L.L. on May 3, 2018, and she confirmed that she had not applied for the credit card and the email account was not hers.
19. 39 emails were exchanged between sgttalbertmill@yahoo.com and patrobertson501@yahoo.com from October 14, 2014 through April 3, 2015. These emails involved the passing of documents containing personal information for thousands of individuals. As an example, on February 26, 2015, patrobertson501@yahoo.com sent an email to sgttalbertmill@yahoo.com that contained an attached document with dozens of individual's personal identifying information to include name, address, date of birth, and social security number. One individual on this list, who will be referred to as B.J., had a

⁷ A preservation request was submitted to Yahoo! Inc. on April 10, 2018 requesting that they preserve all stored communications, records, and other evidence in their possession for 90 days.

fraudulent 2014 tax return filed in her name claiming an \$8,641 refund. This refund was directed to a B.H. family bank account at Subiaco Federal Credit Union. B.J. was interviewed by IRS-CI Special Agents on July 17, 2017, who confirmed that the 2014 tax return was fraudulent.

BACKGROUND CONCERNING EMAIL

20. In my training and experience, I have learned that the provider provides on-line services, including electronic mail ("email") access, to the public. The provider allows subscribers to obtain email accounts at their domain, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the provider. During the registration process, the provider asks subscribers to provide basic personal information. Therefore, the computers of the provider are likely to contain stored electronic communications (including retrieved and un-retrieved email for the provider's subscribers) and information concerning subscribers and their use of the provider's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
21. Subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the provider. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
22. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such

information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

23. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

24. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as

a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. This application seeks a warrant to search all responsive records and information under the control of the provider, who is a provider subject to the jurisdiction of this court, regardless of where the provider has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within the provider's possession, custody, or control.
26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged

IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner.

Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

27. Based on the forgoing, your affiant respectfully requests this Court to issue a search warrant authorizing the search of the email accounts listed in Attachment A, including user names and associated profiles, which are controlled and maintained by the provider, to seize the evidence, fruits, and instrumentalities described in Attachment B, for violations of False Claims for Tax Refund, Theft of Public Money, and Aggravated Identity Theft.

Respectfully submitted,

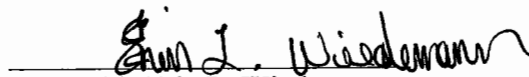


Greg Alexander

Special Agent

IRS Criminal Investigation

Subscribed and sworn to before me on 6/8, 2017.



Honorable Erin L. Wiedemann

United States Magistrate Judge

ATTACHMENT A

ITEMS TO BE SEARCHED AND SEIZED

This warrant applies to all electronically stored data, information, communications, and preserved data contained in, related to, and associated with the Yahoo! email accounts, Yahoo! Inc. User ID, and/or screen names:

- sgttalbertmill@yahoo.com

that is stored at premises owned, maintained, controlled or operated by Oath Holdings Inc., a company headquartered at 701 First Avenue, Sunnyvale, CA 94089.

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by Oath Holdings Inc.

To the extent that information described in Attachment A is within the possession, custody, or control of Yahoo! Inc., including any emails, chats, records, files, logs, or information that has been deleted but is still available to Oath Holdings Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on April 10, 2018, Oath Holdings Inc. is required to disclose the following information, for the period of May 6, 2012 to the present, to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails, messages, and instant messenger communications associated with the accounts, including stored or preserved copies of emails, messages, chats and other communication sent to and from the accounts, draft emails, the source and destination addresses associated with each email, message, chats, or other communication, the date and time at which each email, message, chat or other communication was sent, and the size and length of each email, message, chat, or other communication.
- b. All records or other information regarding the identification of the accounts, to include full customer or subscriber name, customer or subscriber physical address, local and long distance connection records, telephone numbers, and other identifiers, alternate email address, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log

files, and means and source of payment (including any credit or bank account number).

- c. The types of service utilized.
- d. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, files, and all Yahoo! IDS listed on the subscriber's Friends list.
- e. All records pertaining to communications between Yahoo! Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.
- f. All records or other information that were the subject of the preservation request dated April 10, 2018.
- g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to Be Seized by the Government

- 1. All information described above in Section I, including correspondence, records, electronic mail, chat logs, and electronic messages that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 USC § 287, False Claims for Tax Refund, 18 USC § 641, Theft of Public Money, and 18 USC § 1028A, Aggravated Identity Theft, those violations involving unknown individuals and occurring after May 6, 2012, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Evidence regarding the perpetration of any romance scheme, stolen identity refund fraud scheme, or other scheme or artifice to defraud, and the identification and location of the perpetrators, conspirators, and victims of such schemes;
- b. Evidence indicating how and when the Email Accounts and other services were accessed or used, to determine the geographic and chronological context of account/service access, use, and events relating to the crime under investigation and to the Email Accounts owner;
- c. Evidence indicating the Email Accounts owners' and users' state of mind as it relates to the crime(s) under investigation;
- d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- e. Credit card and other financial information including but not limited to bills and payment records;
- f. Evidence of who used, owned, or controlled each account or identifier listed on Attachment A;
- g. Evidence of the times each account or identifier listed on Attachment A was used;
- h. Passwords and encryption keys, and other access information that may be necessary to access each account or identifier listed on Attachment A and other associated accounts.